HUGHES®
An EchoStar Company

SOLUTIONSHEET

Hughes Ransomware and Zero-Day Prevention

Hughes® Ransomware and Zero-Day Prevention, powered by Deep Instinct's advanced deep learning technology, offers a comprehensive endpoint protection solution to combat modern cyber threats. Its proactive, prediction-first approach prevents and responds to known and unknown threats, such as ransomware and zero-day attacks, before they can execute or cause harm. This easy-to-deploy service is ideal for organizations looking to strengthen their cybersecurity defenses while minimizing disruption to daily operations.

The solution utilizes Deep Instinct's AI-driven deep learning engine, which continually learns and adapts to emerging threats. By analyzing vast amounts of data and identifying behavioral patterns, it can predict and block even the most sophisticated attacks, including those that have never been seen before.

Advanced Threat Prevention

Hughes Ransomware and Zero-Day Prevention protects against a wide range of cyber threats, leveraging deep learning to block known and unknown attacks. Traditional signature-based systems rely on databases of known threats, but they are easily bypassed by new, custom, or zero-day attacks. Hughes, on the other hand, uses predictive detection, stopping malicious actions before they can affect systems or steal data.

The solution actively monitors system behavior, detecting ransomware or zero-day exploits by identifying anomalies and suspicious activities that indicate malicious intent. For example, if an attack tries to encrypt files or execute malicious scripts, Hughes detects the abnormal behavior and halts the action in real-time before the threat can escalate.

Fileless and Script-Based Attack Protection

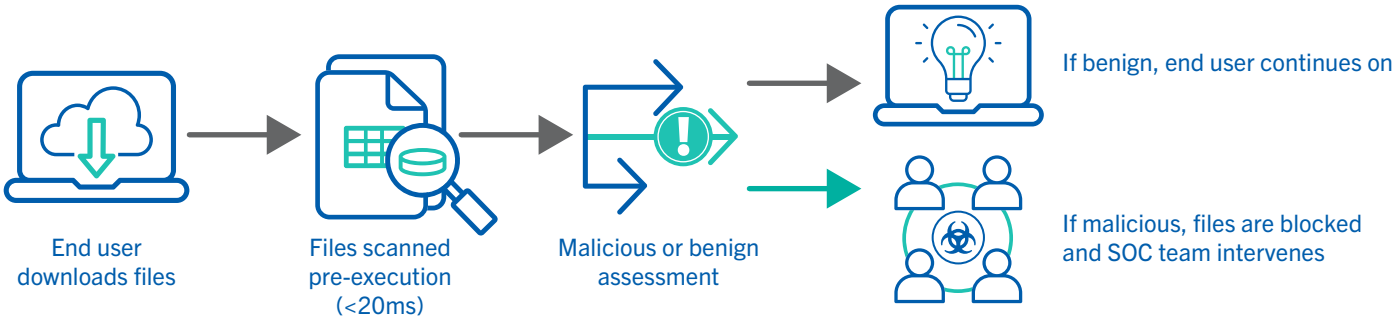
Fileless attacks are particularly challenging for traditional security systems, as they do not rely on files that can be scanned. These attacks often occur entirely in memory, making them difficult to detect and stop. Hughes Ransomware and Zero-Day Prevention excels at identifying and blocking fileless attacks, including those that use PowerShell, MASHTA, JavaScript, and VBScript.

The solution analyzes and blocks malicious scripts before they can execute, whether they are launched via a command line or embedded within legitimate-looking files. This level of protection is critical for defending against modern malware that often uses fileless techniques to evade traditional security measures.

Comprehensive Endpoint Coverage

The Hughes solution is deployed through a lightweight agent installed on endpoints, such as desktops, laptops, mobile devices, and servers. The agent operates with minimal system impact, ensuring that user productivity remains uninterrupted while maintaining high levels of security. It supports a broad range of operating systems, including Microsoft Windows, macOS, Linux, ChromeOS, and Android, making it suitable for diverse IT environments.

Once installed, the agent instantly analyzes potential threats on the endpoint, preventing malware from writing to disks or executing in memory. In case a threat is detected, the solution immediately notifies the 24/7 Security Operations Center (SOC), where analysts review the incident and take action as necessary.



Real-Time Threat Detection and Response

The Hughes 24/7 SOC plays a vital role in providing ongoing protection. As incidents occur, the SOC analysts are alerted and quickly investigate, offering immediate feedback and response to mitigate threats. This real-time analysis helps prevent attacks from spreading and minimizes the impact on the organization.

While the system autonomously blocks threats, the SOC's involvement ensures that any complex incidents are thoroughly handled by cybersecurity experts, providing an additional layer of defense. The result is a rapid response to threats, reducing potential damage and improving the overall security posture of the organization.

Industry-Leading Prevention and Low False Positive Rates

Hughes Ransomware and Zero-Day Prevention boasts an impressive ability to block over 99% of unknown threats, including zero-day and ransomware attacks. This industry-leading protection rate is achieved through the deep learning capabilities of the system, which allows it to predict and block attacks based on behavior rather than relying solely on known threat signatures.

Another critical benefit is the system's low false positive rate of less than 0.1%. This ensures that security teams are not overwhelmed with alerts, allowing them to focus on genuine threats without the distraction of false alarms. The solution is designed to make accurate decisions independently, without the need for cloud-based threat intelligence, making it faster and more reliable.

Simplified Deployment and Integration

Deploying Hughes Ransomware and Zero-Day Prevention is straightforward. The lightweight agent can be quickly installed on customer endpoints, without requiring extensive IT resources or disruption to daily operations. Once deployed, the agent begins protecting the organization immediately, analyzing potential threats and blocking them before they can cause harm.

The solution integrates seamlessly into the existing security infrastructures, providing periodic reporting, incident reviews, and updates through the SOC. Periodic reviews with the SOC analysts ensure that security measures are aligned with the latest threat intelligence, keeping the protection capabilities up to date.

Comprehensive Reporting and Notification

Hughes provides real-time notifications for detected threats. For critical incidents, the system alerts customers by directly calling them to ensure a swift response. Additionally, periodic reports give organizations various insights into their security posture, detailing incidents, and the effectiveness of the security measures in place.

- **Incident Response Notifications:** Alerts are sent via email for all detected threats. For critical incidents, alerts are sent via phone calls to ensure a rapid response time.
- **Periodic Security Reviews:** Regular check-ins with the SOC analysts help keep the security measures aligned with current threat landscapes.

A Key Prevention Tool

Hughes Ransomware and Zero-Day Prevention is a preventative tool that stops threat actors from installing malicious software onto your devices. As a Managed Security Service Provider (MSSP), Hughes adheres to the NIST framework, providing security controls that protect, detect, and respond against modern cyber threats.

Learn more about Hughes Managed Cybersecurity solutions at
www.hughes.com/what-we-offer/managed-cybersecurity/ransomware-zero-day-prevention.

HUGHES
An EchoStar Company
11717 Exploration Lane Germantown, MD 20876 USA
www.hughes.com

H72505 FEB 25